JPAS ACCOUNT MANAGEMENT POLICY

Version 5.0
Date of last update: 1/30/2013

Table of Contents

1. Purpose 3
2. Background 3
3. Organization Roles & Responsibilities 3
   3.1 JPAS Account Manager 3
   3.2 DoD Security Services Center 3
   3.3 Distributed Account Management Process 4
   3.4 Technical Support and Training 4
   3.5 Account Management Support 5
4. Account Lifecycle 5
   4.1 JPAS Account Requirements 5
      4.1.1 System Access Request Form 6
      4.1.2 Letter of Appointment 7
      4.1.3 Mandatory Training Courses 7
   4.2 Appointment of Top Hierarchical Account Managers 8
   4.3 JCAVS Account Activation and Termination 8
   4.4 JAMS Account Activation and Termination 8
   4.5 Account Transfer Between Organizations/Companies 9
   4.6 Unexpected Loss of an Account Manager 9
   4.7 JPAS Accounts for Contractors Working at Government Agencies 9
5. Security 9
   5.1 System Data 9
   5.2 Privacy Act 9
   5.3 Security Banner 10
   5.2 Password/PIN Management 10
   5.3 User IDs 11
   5.4 Account Activity 11
   5.5 Locked Accounts 11

5.6 Misuse of JPAS 12
Acronyms 13
Appendix A: Procedures Governing Use of JPAS by Cleared Contractors 14

JOINT PERSONNEL ADJUDICATION SYSTEM
Account Management Policy

1. Purpose
This policy outlines account management guidance for the Department of Defense (DoD) Joint Personnel Adjudication System (JPAS).

This policy is maintained by the JPAS Program Management Office (PMO) and shall be reviewed at least annually. Program management of JPAS transitioned from Defense Security Services to the Defense Manpower Data Center (DMDC) on June 21, 2010.

Contact information for references mentioned in this policy can be found on the JPAS homepage under Points of Contact.

2. Background
JPAS is the DoD Personnel Security Management System designed to standardize and re-engineer DoD personnel security, achieve interoperability with the Military Services, DoD Agencies, Industry, and Other designated Organizations, and improve data exchange with the DoD Accession community. JPAS provides DoD security personnel access to mission-critical data by offering rapid, reliable, and secure worldwide dissemination of personnel security information.

JPAS consists of the JPAS database, the Joint Clearance Access and Verification System (JCAVS), and the Joint Adjudication Management System (JAMS). While both JCAVS and JAMS provide access to data contained in the JPAS database, JCAVS is designed to provide an interface for the security personnel community and JAMS is designed to provide an interface for DoD adjudicator personnel.

3. Organization Roles & Responsibilities

3.1 JPAS Account Manager
The JPAS Program Manager (PM) is responsible for the formulation of JPAS account management policy, the enforcement of that policy, and the account administration of the top hierarchical primary and alternate Account Managers (AM) for the Services, Unified Commands, DoD Agencies, Industry, and Other Organizations. Services, Unified Commands, DoD Agencies, Industry, and Other Organizations are responsible for the administration and maintenance of JPAS accounts within their Security Management Office (SMO).

3.2 DoD Security Services Center
The DoD Security Services Center provides technical support to all users but only provides account management support to the top hierarchical primary and alternate AMs within Unified Commands, DoD Agencies, Industry, and Other Organizations. Issues or concerns that require the attention of the JPAS PM should be submitted to the DoD Security Services Center. Top hierarchical primary and alternate Military Service AMs should contact their Service JPAS PMO representative for account

management issues or concerns. The Call Center is the JPAS Functional Manager (FM) for Industry and non-DoD agencies.

3.3 Distributed Account Management Process

The function of the Distributed Account Management process is to extend the administration and management of JPAS user accounts across the Military Services, Unified Commands, DoD Agencies, Industry, and Other Organizations. Due to the large number of JPAS customers, the burden of user account management is primarily delegated to top hierarchical AMs within the Military Services, Unified Commands, DoD Agencies, Industry, and Other Organizations. Accountability for JPAS account management is the responsibility of those AMs.

AMs are authorized to manage all applicable JPAS user accounts within their respective SMO. This includes maintaining appropriate paperwork (see section 4.1 below) and providing account management support to their users as set forth in this policy and guidance from the JPAS PMO. Top hierarchical AMs may establish organizational policies to supplement this document; however, those policies may not conflict with this policy document, nor guidance from the JPAS PMO.

An AM may, on occasion, be requested by another DoD organization to manage a local account for that organization as a courtesy. The AM managing another organization's account shall document this request in writing and contact the JPAS PM via the Data Request System (DRS) process for approval of the request. The AM shall then be responsible for maintaining the appropriate paperwork as set forth in this policy for the tenant users. The AM shall be required to provide account management support to the tenant users as set forth in this policy. AMs shall follow any additional guidelines set by their organization for the courtesy management of another organization's account while adhering to any guidance provided by the JPAS PM – if the request is approved.

An account manager is not allowed to manage his or her individual JPAS account. Account managers shall not setup accounts for organizations outside of the DoD without written permission from the JPAS PM via the DRS process.

3.4 Technical Support and Training

JPAS Technical Support is defined as customer support needed to resolve issues concerning user browser configuration, JPAS accessibility via the Internet, and JPAS system malfunctions. Customer support for these technical issues shall be provided primarily via the JPAS PKI Technical Troubleshooting Guide, available on the DMDC JPAS webpages. Users may be required to contact their local area communications or network support for issue resolution. All JPAS users are authorized to contact the Call Center for further technical support requiring immediate resolution due to mission requirements for the aforementioned technical issues. *Support for PK-logon issues is provided solely in the JPAS PKI Technical Troubleshooting Guide and through the JPAS Help Desk email box.*

The Call Center representatives are NOT JPAS trainers. Functional questions must be answered by your respective organization's JPAS PMO or Security Officer.

JPAS instructor led and computer based training is available through the Defense Security Service Center for Development of Security Excellence (CDSE) http://www.dss.mil/seta/index.html. Specific Security Training, Education and Professionalization Portal (STEPP) courses are:

- For JAMS Users: JPAS/JAMS Virtual Training for Security Professionals, STEPP course PS124.06: http://www.dss.mil/cdse/catalog/elearning/PS124.html

- For JCAVS Users: JPAS/JCAVS Virtual Training for Security Professionals, STEPP course PS123.16: http://www.dss.mil/cdse/catalog/elearning/PS123.html

3.5 Account Management Support

JPAS Account Management Support is defined as customer support needed to resolve issues concerning account maintenance, e.g., resetting passwords, locking or unlocking accounts, the top hierarchical primary and alternate AMs within Unified Commands, DoD Agencies, Industry, and Other Organizations.

Only top hierarchical primary and alternate AMs within Unified Commands, DoD Agencies, Industry, and Other Organizations may contact the Call Center directly for account management support. The remainder shall contact the personnel as outlined by their respective Military Service, Unified Command, DoD Agency, Company, and Other Organization—typically the lower hierarchical AMs or appropriate Information Systems support personnel – located on the Points of Contact page of the DMDC JPAS website.

Military Service, Unified Command, DoD Agency, Industry, and Other Organizational top hierarchical primary and alternate AMs shall familiarize themselves with all documentation posted on the DMDC JPAS website in order to provide adequate support for their SMO.

4. Account Lifecycle

4.1 JPAS Account Requirements

Each individual accessing JPAS must have a separate and unique account created by the individual's AM. The account manager must maintain a current record of every JPAS account established. Office accounts shall not be created. Each JPAS account will correspond to a single user who is responsible for all actions taken using that account. JCAVS and JAMS accounts cannot be simultaneously assigned to the same social security number.

Access to the JPAS application shall be granted only if necessary to complete an individual's job duties. In order to receive a JPAS account, a potential user must have a favorable security clearance eligibility determination. JCAVS users, Levels 2, 3 and 8, require at a minimum the favorable adjudication of a SSBI. JPAS users who do not meet the required security clearance requirements cannot be assigned an account. Additionally, eligibility cannot be out of scope unless potential users have submitted all required paperwork for a reinvestigation or their security manager authorizes that the reason for their eligibility being out of scope is due to deployment. If a new JPAS account request is submitted for a person with an ongoing investigation and they already have access [to sensitive information], or they have an interim clearance, their JPAS account request will be approved. Access to JPAS will be suspended for any of the following clearance eligibilities: "Pending Reply to Statement of Reasons," "Denied," "No Determination Made," "Revoked," "Loss of Jurisdiction," or "Action Pending."

Access to JPAS is authorized via means of contractor-issued (for contractors) or government-owned equipment (for government personnel and authorized contractors) with appropriate security controls

in place. JPAS users may not access their accounts from personal or home computers or over unsecured wireless networks. Sharing of user names and passwords or PK-logon credentials is prohibited. Doing so will result in termination of the offender's JPAS account and a technology incident will be recorded on the offender's JPAS record. If you are part of a contract, your contracting office will be notified of the security incident.

Military Service, Unified Command, DoD Agency, Industry, and Other Organizational AMs will create JCAVS accounts for their users and provide account management to those accounts. Accounts shall not be created for personnel outside of your company or outside of the DoD without written permission from USD(I).

A description of the JCAVS user levels and user security clearance requirements can be found in the JPAS General FAQs document, question 3, on the DMDC JPAS home page.

JPAS accounts for non-DoD government agencies are issued by exception. If a non-DoD government agency requests a JPAS account, the agency must have a National Industrial Security Program (NISP) agreement with the Department of Defense for industrial security services. In addition, the non-DoD government agency must formally explain why using the Office of Personnel Management's (OPM) Central Verification System (CVS) database to verify contract clearance information will not meet the needs of the agency, and explicitly state why a JPAS account is necessary. The agencies that have existing agreements with the DoD for industrial security services are listed in the National Industrial Security Program Operating Manual (NISPOM), paragraph 1-103b, and do not include sub-agencies. Lastly, the agencies must follow DMDC policy regarding the management of the account and adhere to the mandatory re-verification of individuals' eligibility requirements on an annual basis.

4.1.1 System Access Request Form

The System Access Request (SAR) Form (link located inside the JPAS Account Request Procedures document on the JPAS homepage) is used to collect information required to grant an account in the JPAS system, to formally document the account request, and to provide accountability for the use of the account. SARs are also used to request account deletions and to make changes to user levels, roles, and permissions.

SARs shall be completed and filed for all Military Service, Unified Command, DoD Agency, Industry, and Other Organizational account managers and users of the JPAS system. SARs shall have the signature of the individual requesting an account, the signature of the nominating official, and signature of the validating official before account access is granted. The nominating official CANNOT be the same as the requestor.

SARs must remain on file for the lifetime of the account, plus six months after the termination of an account. This includes initial SARs submitted to activate an account plus any subsequent SARs submitted to change user levels, roles, and permissions.

Industry Users- Review ISL 04/02 for additional requirements to obtain JPAS accounts for Industry and Appendix A: Procedures Governing Use of JPAS by Cleared Contractors for additional information related to contractors' use of JPAS.

4.1.2 Letter of Appointment

In addition to the SAR form, a Letter of Appointment (LOA) is required for Industry, DoD Agency and Non-DoD Government Agency JPAS account applicants. Military account applicants are not required to submit an LOA at this time.

The LOA should be on your agency's/company's letterhead indicating who the account is for and the specific job duties that require JPAS access. Simply stating "to do my job" is insufficient justification for a JPAS account. Letters will include applicant full names, social security numbers, and contact information (i.e., commercial and DSN work telephones, office addresses, and work email addresses).

Your Agency's Director (or delegate), or a Corporate Officer or Key Management Personnel (KMP) listed in the Industrial Security Facilities Database (ISFD) must sign the letter. The authorization signature on the LOA shall be the same as the authorization signature on the SAR form. Agency delegates must be GS-14 grade (or agency equivalent) or higher. Include the contact information for the Agency Director (or delegate), or Corporate Officer, or KMP making the request (i.e., commercial and DSN work telephones, and office address).

LOAs must remain on file for the lifetime of the account, plus six months after the termination of an account. This includes initial LOAs submitted to activate an account plus any subsequent LOAs submitted to change user levels, roles, and permissions from a normal user role up to an account manager. An LOA is not required if including additional standard user roles (for instance a JCAVS user going from a level 10 to a level 6).

4.1.3 Mandatory Training Courses

As of January 19th 2013, the JPAS disclosure agreement has been modified to include an assertion that the user has "completed the necessary training with regards to Security Awareness and safe-guarding Personally Identifiable Information." These training courses specifically refer to the following programs:

- CyberAwareness Challenge/Security Training (2 options):
  http://iase.disa.mil/eta/cyberchallenge/launchPage.htm
  This includes any organization (service/company/agency) security training the subject may be required to take, such as annual NISP mandatory security training

- Personally Identifiable Information (2 options):
  http://iase.disa.mil/eta/pii/pii_module/pii_module/index.html or,
  http://www.dss.mil/cdse/catalog/elearning/DS-IF101.html

Starting in March 2013, once the new PSSAR form is implemented, new JPAS account requests will need to include proof of completion for these courses. For existing account holders, it is recommended that these certificates (or attendance lists) are maintained at an individual or service/company/agency level on an annual basis. Please note DMDC will not maintain these certificates of completion beyond the new account request procedure; it is up to the

individual/organization to maintain proof of their annual training requirement as it will be requested in the event of a security incident or an audit.

4.2 Appointment of Top Hierarchical Account Managers

Military Services, Unified Commands, DoD Agencies, Industry, and Other Organizations shall appoint their top hierarchical primary and alternate AMs and provide to the JPAS PMO written verification of those appointments. Military Services, Unified Commands, DoD Agencies, Industry, and Other Organizations shall submit to the JPAS PMO an Appointment Letter, on organizational letterhead, and signed by the organization's Head, Commander, Director, or delegate or KMP, naming their top hierarchical primary and alternate AMs. The Appointment Letter may also request removal/deletion of any current top hierarchical primary and alternate AMs whom the Military Services, Unified Commands, DoD Agencies, Industry, and Other Organizations wish to remove from the position. Letters will include AM full names, social security numbers, and contact information (i.e., commercial and DSN work telephones, office addresses, and work email addresses). Letters will also include contact information for the organizational Head, Commander, Director, or designee or KMP making the request (i.e., commercial and DSN work telephones, and office address).

For top hierarchical primary and alternate AMs, an Appointment Letter shall be submitted with the applicable SAR requesting account activation, account deletion, or changes to user levels and permissions. The authorization signature on the SAR shall be the same as the authorization signature on the Appointment Letter. The JPAS AM shall establish and manage accounts for top hierarchical AMs and maintain the accounts, SARs, and Appointment Letters.

Military Services, Unified Commands, DoD Agencies, Industry, and Other Organizations are responsible for sending the JPAS AM a delete SAR form when top hierarchical primary and alternate account managers no longer require access to JPAS.

4.3 JCAVS Account Activation and Termination

Top hierarchical AMs are authorized to establish and manage JCAVS user accounts within their respective SMO/Organization. This includes maintaining appropriate paperwork and providing account management support to their JCAVS users as set forth in this policy. Top hierarchical AMs may establish organizational policies to supplement this document. A SAR and LOA shall be completed and filed for each user of the JCAVS system. The SAR shall have annotated on it the applicable account activation, deletion, or changes to user levels and permissions. Military Service, Unified Command, DoD Agency, Industry, and Other Organizational JCAVS users shall adhere to any additional account management policy requirements set forth by their organization.

4.4 JAMS Account Activation and Termination

SARs and LOAs for Central Adjudication Facility (CAF) adjudicators shall be submitted to their respective CAF AM. CAF AMs shall establish and manage their CAFs' JAMS accounts and maintain the SARs and LOAs.

A SAR and LOA shall be completed and filed for each user of the JAMS system. The SAR shall have annotated on it the applicable account activation, deletion, or changes to user roles and permissions. JAMS users shall adhere to any additional account management policy requirements set forth by their CAF.

4.5 Account Transfer Between Organizations/Companies

JPAS accounts shall NOT be transferred between organizations/companies. If a user or AM leaves an organization/company, the associated account in JPAS must be deleted by the owning organization/company. If JPAS access is required at the new organization/company, a new JPAS account shall be created by the gaining organization/company.

4.6 Unexpected Loss of an Account Manager

Account managers may be unavailable to manage an account for a variety of reasons, e.g., death, incarceration, illness, etc. Establishing contingency responses to the loss of AMs is the responsibility of each Military Service, Unified Command, DoD Agency, Company, and Other Organization.

Each Military Service, Unified Command, DoD Agency, Industry, and Other Organization must have a primary and alternate account manager.

4.7 JPAS Accounts for Contractors Working at Government Agencies

Contractors who perform personnel security management functions as an Information Security Program Manager, Special Security Officer, Special Security Representative, etc., on behalf of a Military Department (MILDEP) or DoD Agency are the responsibility of the hiring MILDEP or DoD Agency. This responsibility includes JPAS account management to include the immediate termination of an individual's JPAS account in the event of any personnel security action such as suspension, revocation, or denial of the access or clearance.

The occurrence of any personnel action annotated in JPAS that is of a punitive nature for a system user and the user's account has not been terminated will result in restrictions to the permissions of the MILDEP or DoD Agency responsible for the contractor.

5. Security

5.1 System Data

Contents of the JPAS system, to include screen images and printed media, contain data that is subject to the Privacy Act of 1974 and must be marked appropriately if printed. Under the Privacy Act of 1974, personnel information retrieved through JPAS must be safeguarded. Disclosure of information is IAW instructions as outlined on the security banner associated with the JPAS system.

5.2 Privacy Act

The Joint Clearance and Access Verification System (JCAVS) within JPAS is intended for use by security managers/security officers to update other JCAVS users with pertinent personnel security clearance access information in order to ensure the reciprocal acceptance of clearances throughout DoD.

Its intended use, according to policy, does not include giving out the JCAVS records to the subject of record for their personal use without a proper Privacy Act request or authorization from the record owner.

JCAVS contains not only clearance eligibility information but also Investigative Summary and Adjudication Summary information as well as Incident Reports, some of which may have originated with a third agency requiring their review/comments before a disclosure is made. Therefore, DMDC does not authorize the direct disclosure of JCAVS records by a security manager to the Subject of

record. Service schools requiring clearance verification can either request JCAVS access themselves or have the user agency provide to them subject's clearance verification.

5.3 Security Banner

This is a Department of Defense (DoD) Computer System. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) is provided for official government use only and is not open to the public. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. DoD computer systems may be monitored for all lawful purposes, including to ensure their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Unauthorized attempts to upload, download or change information on this system is strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987, the National Information Infrastructure Protection Act of 1996, and United States Code Title 18, section 1030.

DoD policy prohibits the use of web technology which collects user-identifying information such as extensive lists of previously visited sites, e-mail addresses, or other information to identify or build profiles on individual visitors to DoD publicly accessible web sites. DoD policy, however, does permit the use of "cookies" or other web technology to collect or store non-user identifying information but only if users are advised of what information is collected or stored, why it is being done, and how it is to be used. This policy will be clarified to make clear that "persistent cookies" (i.e., those that can be used to track users over time and across different web sites) are authorized only when there is a compelling need to gather the data on the site; appropriate technical procedures have been established to safeguard the data; and the Secretary of Defense has personally approved use of the cookie.

5.2 Password/PIN Management

The JPAS system default password shall be randomly generated by the system and provided to the account manager at the time an account is created or a password change is forced. The account manager shall relay, via encrypted email, the randomly generated password to the user.

Passwords are used to self-register non-CAC certificates to a user's JPAS account. A user will have to remember their username and password in order to self-register their non-CAC certificates. After registering your certificates using your username and password, you will not be required to change your password. Note – you will need to register your certificates each time you get new certificates, or when switching between different certificates for the same user.

The JPAS system will lock a user ID after three consecutive failed attempts at the self-registration screen. JPAS user accounts shall be unlocked only by the appropriate JPAS AMs.

The JPAS PM and Call Center have the ability to force password changes for account managers within JPAS. JCAVS and JAMS AMs have the ability to force password changes within JPAS for their organization's users.

PINs are 6 digit numeric codes associated with your PK credentials and are managed differently depending on the specific type of credential used:

- For a DoD CAC, you have 3 attempts to enter a correct PIN. If you fail on the 3rd attempt, your credential will be locked. In order to unlock your credentials, you will need to visit a DEERS/RAPIDS station to unlock and subsequently use.
- For a Federal PIV, contact the issuer of the PIV for their reset policies.
- For ECA and other DoD approved PKI credentials, this process can vary from issuer to issuer. Note: some issuers do not conduct a PIN/Password reset and will require the purchase of a separate credential. Please be forewarned and ask the vendor's SOP prior to purchase.

JPAS users may never share their user names, passwords, PK certificates, PINs, or other authentication information with any other individual, including anyone who is a designee or an alternate to the account holder. JPAS does not have "company account." Sharing of user names and passwords is prohibited. Doing so will result in the termination of the account and a technology incident will be recorded on the offender's JPAS record.

Violations of the procedures will lead to the termination of the JPAS account, or exclude culpable companies or persons from access to JPAS for a specified or indefinite period. Information concerning violations of these procedures may also be referred to other federal agencies for consideration of administrative, civil or criminal sanctions when circumstances warrant.

If the company with the security violation has a requirement that JPAS access is needed, DMDC will reinstate a JPAS account to an individual associated with the company, other than the individuals who have violated DoD Regulations. DMDC requires a written request from your company's Government Sponsor on their appropriate letterhead. The written request will need to acknowledge that the Government Sponsor is aware a JPAS security violation has occurred with this company and is requesting JPAS access to be given to another individual in order to support mission-critical and job-essential tasks. Once DMDC has received all the requested information, JPAS access can be granted.

5.3 User IDs

JPAS User IDs are systematically generated at account creation and are unique to individuals. Group login accounts and the sharing of User IDs are prohibited.

5.4 Account Activity

An active JPAS account is one that has been logged into in the past 30 days. An inactive JPAS account is an account that has not been logged into in the past 60 days. If a JPAS account is inactive—i.e., not successfully accessed—for more than 60 days, the JPAS system shall automatically lock the account. The AM managing the account will be able to unlock the account, unless the account exceeds 90 days of inactivity. JPAS accounts that have not been logged into for longer than 90 days are deleted per DoD Regulations (APP6240). If an account is needed, a new account will have to be established following the aforementioned guidelines.

5.5 Locked Accounts

Account managers may only unlock accounts for users within their SMO. Do not unlock accounts that have been locked by an Administrator unless you have permission from the locking Administrator.

Contacts

Name	Contact Information
JPAS Program Management Office JPAS Program Manager	JPAS PMO Defense Manpower Data Center 400 Gigling Road, Seaside, CA 93955
DoD Security Services Center	1 (888) 282-7682 FAX: (703) 493-8965 E-mail (SAR-related Correspondence): account.request@dsshelp.org E-mail (All Other Correspondence): call.center@dsshelp.org Website

5.6 Misuse of JPAS

By clicking the "I agree" consent box on the DoD Security Banner page in the JPAS application, users are consenting to the terms of use of the application and are agreeing to maintain compliance with the Privacy Act of 1974 and all applicable JPAS rules and regulations, including this Account Management Policy. Violations of this Account Management Policy constitute a misuse of JPAS and will result in termination of the offender's JPAS account, and may include disallowing culpable companies or persons from future access to JPAS, and/or recording of an incident on the offender's JPAS record. Information concerning violations of these procedures may also be referred to other federal agencies for consideration of administrative, civil or criminal sanctions when circumstances warrant.

Common misuses of JPAS include, but are not limited to:

- Sharing of username, password, CAC or PIV cards and/or associated PIN numbers to access the system.
- Allowing non-cleared individuals to access the system.
- Leaving the JPAS application insecure while logged into it.
- Allowing others to view data on the JPAS screen that do not have the proper authorization.
- Providing printouts of JPAS data without proper authorization.
- Querying the JPAS application for 'celebrity' records.
- Querying the JPAS application for your own record.

Acronyms

AM	Account Managers
CAF	Central Adjudication Facility
DoD	Department of Defense
JAMS	Joint Adjudication Management System
JCAVS	Joint Clearance Access and Verification System
LOA	Letter of Appointment
MILDEP	Military Department
JPAS	Joint Personnel Adjudication System
PM	Program Manager
PMO	Program Management Office
SAR	System Access Request
JUA	JPAS User Agency- if term is used

Appendix A: Procedures Governing Use of JPAS by Cleared Contractors

National Industrial Security Program Operating Manual (NISPOM) paragraph 2-200b states that "When the CSA [Cognizant Security Agency] has designated a database as the system of record for contractor eligibility and access, the contractor shall be responsible for annotating and maintaining the accuracy of their employees' access records. Specific procedures will be provided by the CSA." The Department of Defense, acting as a CSA, has designated the Joint Personnel Adjudication System (JPAS) as the DoD system of record for contractor eligibility and access.

JPAS is a U.S. Government information system that contains official government records. The information in JPAS must be protected from unauthorized disclosure and used only for authorized purposes. Contractors may only use their JPAS accounts to manage the access records of their employees and consultants, and to verify the access levels and affiliations (e.g., employee of ABC Company) of incoming visitors who require access to classified information.

The following procedures are issued under the authority provided by NISPOM paragraph 2-200b. Contractors shall follow these procedures when using JPAS and shall ensure that authorized users of JPAS have been properly informed about these procedures and any other specific policies governing access to and use of JPAS.

1. Contractors shall accurately maintain the JPAS records pertaining to their employees and consultants. Contractors must expeditiously update these records when changes occur (e.g., termination of employment).

2. Contractors are prohibited from placing false information in JPAS, and DMDC will seek appropriate sanctions against contractors and contractor employees who knowingly place false information in JPAS.

3. DoD issues JPAS accounts exclusively for use by a specific contractor or corporate family of contractors. Persons given access to JPAS as account holders may only use JPAS on behalf of the cleared contractor or corporate family of contractors through which the account was issued. For example, an employee of ABC Company holding a JPAS account issued through ABC Company and who works at a government site is not authorized to use the contractor-granted account in support of the government customer. If the government customer requires the contractor employee to review or update JPAS records on behalf of the government customer, the government customer must provide a separate, newly created JPAS account for the contractor employee to use – they may not share an existing user ID and password.

4. The JPAS account manager must be a company employee. The JPAS account manager cannot be a subcontractor or consultant.

5. Contractors may subcontract or obtain consultant support for administering security services, not account management as stipulated in #4 above. The using contractor will provide a JPAS account to the subcontractor or consultant under the using contractor's Security Management Office (SMO) for the sole purpose of permitting the subcontractor or consultant to provide security services for the using company. Subcontractors or consultants providing such security services must be under the direct supervision of the using contractor's FSO or FSO's designee.

6. Each individual accessing JPAS must have a separate and unique account created by the individual's JPAS account manager. The account manager must maintain a current record of every JPAS account established as per JPAS Account Management Policy, Section 4.2: System Access Request Form.

7. JPAS users may never share their user IDs, passwords, PK certificates, PINs, or other authentication information with any other individual, including anyone who is a designee or an alternate to the account holder.

8. Access to JPAS is only authorized by means of company or government-owned equipment with appropriate security controls in place. JPAS users may not access their accounts from personal or home computers or over unsecured wireless networks.

9. Contractors are not permitted to change an existing date notation in JPAS for the Classified Information Nondisclosure Agreement (SF 312). Contractors must, however, input the date that the SF 312 was signed when JPAS does not reflect a date.

10. Contractors are authorized to verify prospective employees' eligibility for access to classified information in JPAS prior to an offer of employment being extended. However, contractors may not use JPAS for recruiting purposes.

11. While access to JPAS is only granted to contractors who have a legitimate need for such access in support of classified work being performed for the Government, JPAS is not a classified system. DSS will not grant a facility security clearance (FCL) for the sole purpose of allowing a company or its employees to gain access to JPAS.

12. Any contractor with JPAS access that becomes aware of a violation of these procedures shall immediately report the nature of the violation, the names of the responsible parties, and a description of remedial action taken, to the servicing DSS Industrial Security Representative.

NOTE: Violations of the procedures may lead DMDC to suspend or withdraw JPAS access, terminate the JPAS account, mark a technology incident on a user's JPAS record, or exclude culpable companies or persons from access to JPAS for a specified or indefinite period. DSS will also refer information concerning violations of these procedures to other federal agencies for consideration of administrative, civil or criminal sanctions when circumstances warrant.